REMARKS

This Amendment is submitted in response to the Examiner's Action mailed October 23, 2002, with a shortened statutory period of three months set to expire January 23, 2003.

Applicants claim a method, system, and product for securing a transaction in order to prevent fraudulent transactions. Applicants claim the smart card being initialized by a credit card issuer by storing a secret master key and client information on the card. A copy of this master key is also stored within the credit card issuer. The master key is associated with the client information. The master key is kept secret. A digest is created by the smart card using the client information and the master key. This digest is then sent to the credit card issuer.

The credit card issuer then generates its own digest using the copy of the master key stored by the credit card issuer and the client information. If the digest generated by the credit card issuer matches the digest sent by the merchant, the transaction is authorized.

The Examiner rejected to claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,317,636 issued to *Vizcaino*, in view of U.S. Patent 5,530,232 issued to *Taylor* and U.S. Patent 5,850,446 issued to *Berger*. This rejection is respectfully traversed.

Vizcaino describes a smart card that includes an ever-changing verification number. This number is then encrypted and sent to the computer which is to verify the transaction. The smart card and the computer both keep a copy of the verification number. They both increment their numbers after each transaction. After receiving an encrypted number, the computer decrypts the received encrypted number. The computer then compares the decrypted number to its stored number. If they match, the transaction is approved. This verification number is the only thing used by *Vizcaino* to authenticate the transaction.

Further, the verification number is not kept secret by *Vizcaino*. In fact, *Vizcaino* teaches away from keeping this number secret. The number is displayed in a window by the card, and is thus very easily obtained.

Applicants describe using a secret master key as well as client information to create the digest that the smart card sends to the credit card issuer. The credit card issuer uses this digest to authenticate the transaction. If the master key is publicly available and not secret, the master key is of no use in the authentication process. If anyone can easily obtain the master key, the credit card issuer would not be able to verify that the transaction is not fraudulent.

In addition, the master key claimed by Applicants does not change over time. The verification code described by *Vizcaino* changes after each transaction. This verification number must change after each transaction because the number is made public.

Vizcaino does not describe, teach, or suggest a digest. It does not describe, teach, or suggest using a secret master key and client information to create a digest. It does not describe, teach, or suggest a master key that remains unchanged.

Taylor describes a multi-application smart card. *Taylor* does not describe the smart card creating a digest. *Taylor* does not describe the smart card creating a digest using a secret master key and client information, where a copy of the master key is kept by the credit card issuer that initialized the smart card by storing the master key on the smart card.

Berger describes a customer computer transmitting a digest to a payment computer. The purpose of this digest is to ensure that the data that accompanies the digest has not been changed during its transmission. "Message digests help verify that a message has not been altered because altering the message would change the digest." See Column 16, lines 31-33.

The digest is created by *Berger* using public keys. By definition these keys are publicly available. *Berger* teaches away from using a secret key to create the digest. The digest is then encrypted by the merchant's private key. However, the digest itself is created using the public keys.

Therefore, *Berger* does not describe, teach, or suggest creating a digest using a secret master key. *Berger* does not describe, teach, or suggest the master key being stored by the credit card issuer. *Berger* does not describe, teach, or suggest the key used to create the digest of *Berger* being associated with client information.

The Examiner states that the teachings of *Berger* could be applied to a smart card. Applying the teachings of *Berger* to a smart card does not render Applicants' claims unpatentable. The digest of *Berger* does not help prevent fraudulent transactions. It helps ensure that a transmitted message is not altered during transmission. Combining the digest of *Berger* with a smart card would only ensure that the data transmitted from the smart card was received unchanged by the receiver.

It is respectfully urged that the subject application is patentable over *Vizcaino*, *Taylor*, and *Berger* in combination and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 01/23/2003

Respectfully submitted,

Lisa L.B. Yociss
Reg. No. 36,975
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants

REDACTED CLAIMS:

1. (Amended) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;

receiving a request for a digest from a requestor;

retrieving the [a] master key;

retrieving unique client information;

the client information being associated with the master key;

creating the digest by hashing the unique client information and the master key; and

returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the [a] third party.

8. (Amended) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

receiving, into the [a] smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving unique client information, from the smart card memory;

retrieving [a] the master key, the master key being known to the [a] credit card issuer;

creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing the billing digest, the unique merchant information and the unique client information to the requestor.

11. (Amended) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

sending a data transmission to the [a client's] smart card, wherein the data transmission includes unique merchant information and a request for a billing digest;

receiving the billing digest, the unique merchant information and unique client information from the [client's] smart card, the billing digest being hashed from the unique merchant information, unique client information and the master key [secret information] from the [client's] smart card; and

transmitting the unique merchant information and unique client information from the [client's] smart card to a credit card issuer.

13. (Amended) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged, and is not altered after the transaction, the third party storing a copy of the master key within the third party, the master key being kept secret;

receiving, by the third party, a transaction request from a requestor, wherein the request includes a digest and unique client information;

the client information being associated with the master key;

accessing [a] the copy of the master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the copy of the master key;

comparing, by the third party, the authorization digest with the digest from the requestor; and

returning a response to the requestor from the third party, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor.

19. (Amended) The method recited in claim 13 above, wherein the third party is a credit card issuer, the transaction is a credit card transaction and the requestor is a merchant, further wherein the requestor information includes information describing at least one of a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

20. (Amended) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key;

receiving the master key from a credit card issuer upon an initialization of the smart card by the credit card issuer, the master key being associated with the customer information;

creating an authentication digest by the credit card issuer, wherein the authentication digest is hashed from the merchant information, customer information and a master key associated with the customer information;

comparing the authorization digest with the billing digest; and

authorizing a transaction based on the comparison of the authorization digest with the billing digest.

22. (Amended) A smart card for conducting secure transactions in order to prevent fraudulent transactions comprising:

a input/output mechanism;

a processor; and

a memory containing:

financial account information;

a secret master key received upon initialization of the smart card, the master key remaining unchanged throughout the use of the smart card, the master key being received from a third party;

functional hashing algorithm;

an executable application, for executing on the processor, for invoking the functional hashing algorithm, wherein the functional hashing algorithm creates a digest from the financial account information and the master key and further wherein the executable application transmits, via the input/output mechanism, the digest and the financial account information to a requestor for approval by the third party.

23. (Amended) A system for conducting secure transactions in order to prevent fraudulent transactions comprising:

a client smart card for creating a billing digest from a resident client information, a resident secret master key and imported merchant information;

the master key being received from a financial institution upon initialization of the smart card, the master key remaining unchanged after use of the smart card, the master key being kept secret, and the master key being associated with the resident client information;

a merchant system for requesting the billing digest and for passing secure transaction information and the billing digest to the [a] financial institution, wherein the transaction information comprises the client information, and the imported merchant information; and

[a] the financial institution for receiving the transaction information and billing digest and for authorizing a transaction by:

accessing a master key stored within the financial institution based on the client information;

creating an authorization digest from the master key stored in the financial institution , the client information and the merchant information; and

comparing the authorization billing digest with the billing digest.

24. (Amended) A system for securing a transaction in order to prevent fraudulent transactions comprising:

receiving means for receiving a secret master key from a third partition prior to the transaction, the master key remaining unchanged after the transaction, the master key being kept secret;

receiving means for receiving a request for a digest from a requestor;

retrieving means for retrieving [a] the master key;

retrieving means for retrieving unique client information;

the client information being associated with the master key;

creating means for creating the digest by hashing the unique client information and the master key; and

returning means for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the [a] third party.

32. (Amended) A system for securing a transaction in order to prevent fraudulent transactions comprising:

providing means for providing from a third party a secret master key to a client, the master key remaining unchanged after the transaction;

receiving means for receiving a transaction request from a requestor, wherein the request includes a digest and unique client information, the digest being created utilizing the master key provided to the client and the unique client information;

the unique client information being associated with the master key;

accessing means for accessing, by the third party, a master key stored within the third party based on the unique client information;

creating means for creating an authorization digest by hashing the unique client information and the master key;

comparing means for comparing the authorization digest with the digest from the requestor; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the authorization digest with the digest from the requestor.

39. (Amended) A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

providing instructions for providing from a third party a secret master key, the master key remaining unchanged after the transaction;

receiving instructions for receiving a request for a digest from a requestor;

retrieving instructions for retrieving the [a] master key;

retrieving instructions for retrieving unique client information;

the master key being associated with the client information;

creating instructions for creating the digest by hashing the unique client information and the master key; and

returning instructions for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with [a] the third party.

40. (Amended) A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

initializing instructions for initializing a smart card by receiving within the card a secret master key from a credit card issuer;

receiving instructions for receiving, into [a] the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving instructions for retrieving unique client information, from the smart card memory;

the unique client information being associated with the master key;

retrieving instructions for retrieving [a] the master key, the master key being provided by the [known to a] credit card issuer;

creating instructions for creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing instructions for passing the billing digest, the unique merchant information and the unique client information to the requestor.